

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-218837

(43)Date of publication of application : 19.08.1997

(51)Int.Cl.

G06F 13/00

G06F 12/14

H04L 12/24

H04L 12/26

(21)Application number : 08-022780

(71)Applicant : HITACHI LTD

(22)Date of filing : 08.02.1996

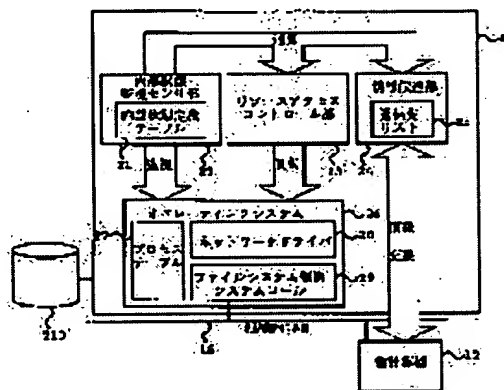
(72)Inventor : KAYASHIMA MAKOTO
TERADA MASATOSHI

(54) NETWORK SECURITY SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize a dynamic access and to improve the security for an intrusion by performing the protective processing of the internal resource related to an abnormality when the occurrence of the abnormality is detected by an internal state monitoring means.

SOLUTION: An internal state monitoring sensor part 22 monitors an operating system 26. When an abnormality is detected, a resource access control part 23 executes an access control processing for the operating system 26 and an information transmission part 24 notifies the other computer 12 entered in a communication destination list 25 of the detection of the abnormality via a private LAN 16. When the detection of the abnormality is notified to a computer 11 from the other computer 12, the information transmission part 24 notifies the resource access control part 23 of the detection of the abnormality in the other computer after the part 24 confirms whether the other computer 12 of a transmission origin is entered in the communication destination list 25 or not.



LEGAL STATUS

[Date of request for examination] 28.02.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3165366

[Date of registration] 02.03.2001

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-218837

(43) 公開日 平成9年(1997)8月19日

(51)Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 13/00	3 5 1		G 0 6 F 13/00	3 5 1 Z
	12/14	3 2 0	12/14	3 2 0 A
H 0 4 L 12/24		9466-5K	H 0 4 L 11/08	
12/26				

審査請求 未請求 請求項の数11 O L (全 14 頁)

(21) 出願番号 特願平8-22780

(22) 出願日 平成8年(1996)2月8日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 萱島 信

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 寺田 真敏

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 弁理士 富田 和子

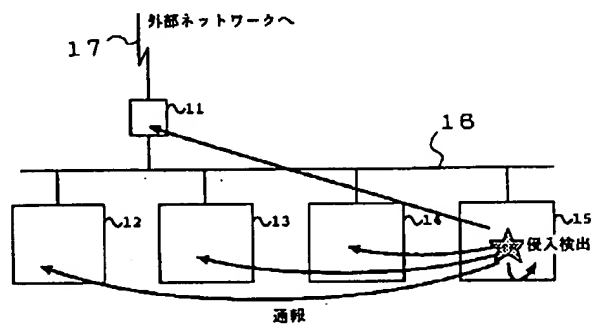
(54) 【発明の名称】 ネットワークセキュリティシステム

(57) 【要約】

【課題】 ネットワークに接続された計算機システムにおいて、組織外からの侵入者に対して個々の計算機のセキュリティを強化する。

【解決手段】 ファイアウォール内の個々の計算機で、起動しているプロセスの個数、ネットワークインタフェースのトラフィック、特定ファイルのアクセス状況等の内部状態を監視することにより、侵入検出を行ない、異常と判断した場合に、自計算機のリソースアクセスの制御および、ファイアウォールを含む他計算機への侵入の通知を行なう。これにより、自組織内の計算機リソースの保護を行なうことができる。特にファイアウォールに対して侵入検出を通知することにより、自組織全体の計算機リソースの保護を一括して行なうこともできる。

図 1



【特許請求の範囲】

【請求項1】 ネットワークに接続された計算機を有するネットワークセキュリティシステムであって、

前記計算機は、

計算機の内部状態を監視し、異常の発生を検知する内部状態監視手段と、

内部のリソースに対するアクセスの制御を行うアクセス制御手段とを備え、

該アクセス制御手段は、前記内部状態監視手段により異常の発生が検知されたとき、当該異常に関連した内部のリソースの保護処理を行うことを特徴とするネットワークセキュリティシステム。

【請求項2】 前記計算機は、前記内部状態監視手段により異常の発生が検出されたとき、前記ネットワークに接続された他の計算機へその旨通知するとともに、前記他の計算機からの異常の発生の通知を受信する情報伝達手段を備え、前記アクセス制御手段は、他の計算機からの異常の発生の通知を受信したときも当該異常に関連した内部のリソースの保護処理を行うことを特徴とする請求項1記載のネットワークセキュリティシステム。

【請求項3】 外部ネットワークに接続された内部ネットワークにおいて、該内部ネットワークに接続された計算機において、該計算機の内部状態の監視処理を行ない、該監視処理により前記外部ネットワークからの侵入を検出すると、アクセス制御による計算機リソースの保護処理と、前記内部ネットワークの他の計算機への検出内容の通知処理とを行なうことを特徴とするネットワークセキュリティシステム。

【請求項4】 前記内部ネットワークに接続された計算機は、前記内部ネットワーク内の他の計算機からの通知待ち処理を行ない、前記外部ネットワークからの侵入の通知を受けると、アクセス制御による計算機リソースの保護処理を行なうことを特徴とする請求項3記載のネットワークセキュリティシステム。

【請求項5】 ネットワークに接続した計算機において、計算機の内部状態の監視処理および、周囲の計算機からの通知待ち処理を行ない、前記ネットワーク外部からの侵入を検出すると、前記ネットワーク内の周囲の計算機とお互いに通知し合うことにより、連係して侵入対策を行なうことを特徴とするネットワークセキュリティシステム。

【請求項6】 前記計算機は、実行プロセスの数と、ネットワークインタフェースのトラフィックと、重要なファイルへのアクセスの少なくとも1つを監視し、該監視の結果が、予め定めた制限内容から外れる場合に、異常が発生したと判断する請求項1～5のいずれかに記載のネットワークセキュリティシステム。

【請求項7】 前記計算機において、監視による異常の検出状況に応じて、段階的にアクセス制御を実施することにより計算機リソースの保護を行なうことを特徴とする

請求項1～6のいずれかに記載のネットワークセキュリティシステム。

【請求項8】 前記計算機において、監視の結果得られたデータと、あらかじめテーブルに登録しておいた計算機の内部状態データとを比較することにより、前記異常として外部からの侵入を判定することを特徴とする請求項1～7のいずれかに記載のネットワークセキュリティシステム。

【請求項9】 前記テーブルの内容をユーザが決定することを特徴とする請求項8記載のネットワークセキュリティシステム。

【請求項10】 前記計算機において、前記テーブルの内容の更新時に、他の計算機に上記テーブルの内容を通知し、他の計算機は上記通知内容に基づき、自己のテーブルの内容を更新することを特徴とする請求項9記載のネットワークセキュリティシステム。

【請求項11】 ネットワークに接続した計算機において、複数のサーバが連動することにより動作するサービスが稼働しているネットワークシステムに対して、連係して侵入対策を行なうと共に、侵入対策に応じて連動サービスの動作を変更することを特徴とする請求項2記載のネットワークセキュリティシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワークに接続した計算機のセキュリティに係わり、特に計算機とファイアウォールが連係して組織外からの侵入者に対する防御を実行するネットワークセキュリティシステムに関する。

【0002】

【従来の技術】 従来、ネットワークを経由した計算機への侵入に対する防御策として、外部とのアクセスに制限を施すファイアウォール（firewall）が提案されている。ファイアウォールは、送信元と送信先のIPアドレスの組合せによりアクセス制御を施すもので、

（1）サービス毎にリソースにアクセスできるIPアドレスを制限し、（2）アクセス記録を残す機能を持つものが主流である。このなかで、チェックポイント（Checkpoint）社の製品であるFirewall-1は、ゲートウェイだけでなく、各計算機もそれぞれアクセス制御を行なう機能を持ち、各計算機の設定は1台の計算機で管理できるようになっている。

【0003】

【発明が解決しようとする課題】 インターネットの発展により、世界中で発信している情報を手元の計算機でリアルタイムに入手できるようになった反面、自計算機も外部からの侵入者の脅威にさらされることになった。このような侵入者に対する防御策として、（1）サービス毎にリソースにアクセスできるIPアドレスを制限し、（2）アクセス記録を残す、ゲートウェイ（狭義のファ

3

ファイアウォール) が提案されている。狭義のファイアウォールを使用することにより、管理者が監視する範囲を限定することができる。しかし、個々の計算機は逆にチェックが甘くなるため、万が一ファイアウォールをすり抜けて侵入されると、その侵入された計算機を足掛かりにして周囲の計算機に攻撃を仕掛けられる可能性がある。前述したCheckpoint社のFirewallは、狭義のファイアウォール以外に、(1) サービス毎にリソースにアクセスできるIPアドレスの制限を各計算機単位で行ない、(2) アドレス制限の設定はリモートで実施することにより、1台の計算機でその設定作業を行なうことができる、という特徴を持っている。しかし、アクセス制御の設定は静的に定義するものであり、一度侵入された場合には管理者がファイアウォールと各計算機に対して対策を施す必要があった。

【0004】そこで本発明では、(1) ファイアウォール内の個々の計算機で侵入の検出を行ない、(2) その結果を周囲にフィードバックする仕組みを提供することにより、動的なアクセスを実現し、侵入に対するセキュリティを高めることを目的とする。

【0005】

【課題を解決するための手段】 上記課題を解決するために、本発明は、ネットワークに接続された計算機を有するネットワークセキュリティシステムであって、前記計算機は、計算機の内部状態を監視し、異常の発生を検知する内部状態監視手段と、内部のリソースに対するアクセスの制御を行うアクセス制御手段とを備え、該アクセス制御手段は、前記内部状態監視手段により異常の発生が検知されたとき、当該異常に関連した内部のリソースの保護処理を行うことを特徴とするネットワークセキュリティシステムを提供する。

【0006】前記計算機は、好ましくは、前記内部状態監視手段により異常の発生が検出されたとき、前記ネットワークに接続された他の計算機へその旨通知するとともに、前記他の計算機からの異常の発生の通知を受信する情報伝達手段を備え、前記アクセス制御手段は、他の計算機からの異常の発生の通知を受信したときも当該異常に関連した内部のリソースの保護処理を行う。

【0007】本発明は、他の見地によれば、外部ネットワークに接続された内部ネットワークにおいて、該内部ネットワークに接続された計算機において、該計算機の内部状態の監視処理を行ない、該監視処理により前記外部ネットワークからの侵入を検出すると、アクセス制御による計算機リソースの保護処理と、前記内部ネットワークの他の計算機への検出内容の通知処理とを行なうことを特徴とするネットワークセキュリティシステムを提供する。

【0008】前記内部ネットワークに接続された計算機は、好ましくは、前記内部ネットワーク内の他の計算機からの通知待ち処理を行ない、前記外部ネットワークか

4

らの侵入の通知を受けると、アクセス制御による計算機リソースの保護処理を行なう。

【0009】本発明は、さらに他の見地によれば、ネットワークに接続した計算機において、計算機の内部状態の監視処理および、周囲の計算機からの通知待ち処理を行ない、前記ネットワーク外部からの侵入を検出すると、前記ネットワーク内の周囲の計算機とお互いに通知し合うことにより、連係して侵入対策を行なうことを特徴とするネットワークセキュリティシステムを提供する。

【0010】前記計算機は、実行プロセスの数と、ネットワークインタフェースのトラフィックと、重要なファイルへのアクセスの少なくとも1つを監視し、該監視の結果が、予め定めた制限内容から外れる場合に、異常が発生したと判断することができる。

【0011】前記計算機において、監視による異常の検出状況に応じて、段階的にアクセス制御を実施することにより計算機リソースの保護を行なうことも可能である。

【0012】前記計算機において、監視の結果得られたデータと、あらかじめテーブルに登録しておいた計算機の内部状態データとを比較することにより、前記異常として外部からの侵入を判定することができる。このテーブルの内容は、ユーザが決定することができる。

【0013】前記計算機において、前記テーブルの内容の更新時に、他の計算機に上記テーブルの内容を通知し、他の計算機は上記通知内容に基づき、自己のテーブルの内容を更新するようにしてもよい。

【0014】また、ネットワークに接続した計算機において、複数のサーバが連動することにより動作するサービスが稼働しているネットワークシステムに対して、連係して侵入対策を行なうと共に、侵入対策に応じて連動サービスの動作を変更することも可能である。

【0015】本発明のネットワークセキュリティシステムでは、組織内の個々の計算機がそれぞれ侵入を検出する処理と、侵入を検出した場合に計算機リソースの保護処理および、周囲の他計算機に対する通知処理を行なうことにより、外部からの侵入に対してセキュリティを強化すると共に、管理者に対して侵入を早期に伝達することができる。

【0016】

【発明の実施の形態】 本発明の一実施の形態を、図1から図10を用いて説明する。図1は、本発明を適用したネットワークセキュリティシステムの全体構成を示す図である。11はファイアウォールとしての計算機、12から15は組織内LAN16に接続された計算機、17はファイアウォール11と外部ネットワークとの接続を行なう専用線である。例えば、計算機15において、外部からの不当な侵入を検出した場合には、後述するようなアクセスコントロール制御処理を自計算機において実

5

行するとともに、組織内LAN16に接続された他の計算機11、12～14へ不当な侵入の発生を通知する。この通知を受けた計算機においても、アクセスコントロール制御処理を行う。

【0017】図2は、図1のネットワークセキュリティシステムで使用する計算機11の概要を示す図である。21は内部状態定義テーブル、22は内部状態監視センサ部、23はリソースアクセスコントロール部、24は情報伝達部、25は通知先一覧リスト、26はオペレーティングシステム、27はプロセステーブル、28はネットワークドライバ、29はファイルシステム制御システムコール、210は外部記憶装置である。

【0018】内部状態監視センサ部22は、オペレーティングシステム26を監視し、監視結果を内部状態定義テーブル21の内容と比較することにより侵入を検出する。内部状態監視センサ部22で異常が検出されると、リソースアクセスコントロール部23および情報伝達部24に通知され、リソースアクセスコントロール部23はオペレーティングシステム26に対してアクセスコントロール制御処理を実行し、情報伝達部24は通信先リスト25に記載されている他計算機12に対して異常を検出したことを組織内LAN16を経由して通知する処理を実行する。アクセスコントロール処理の内容については後述する。また、他計算機12から異常を検出したことが計算機11に通知されてきた場合、情報伝達部24は送信元の他計算機12が通信先一覧リスト25に記載されているか確認した後、リソースアクセスコントロール部23に他計算機での異常の検出を通知し、リソースアクセスコントロール部23はオペレーティングシステム26に対してアクセスコントロール処理および、

実行中のジョブに対する制御を実行する。「実行中のジョブに対する制御」は、例えばUNIXシステムの場合、管理者の権限で実行中のプロセスを終了させることや、プロセスの優先度を変更することに相当する。具体的には、計算機の負荷を異常に重くするジョブを実行しているユーザのプロセスを終了、もしくはその優先度を下げることにより、他のサービスを続行することが可能になる。

【0019】次に、図2の計算機11で用いられるテーブルおよび送信メッセージの構成について図8、図9、および図11により説明する。

【0020】図8は計算機11の内部状態定義テーブル21の構造の一例を示した図である。81はプロセス数定義テーブルであり、計算機11のユーザIDを記述するユーザIDフィールド82と、各ユーザ毎のプロセス数制限値を記述するプロセス数制限値フィールド83により構成されるレコードの集まりである。84はパケット数定義テーブルであり、計算機11と通信可能なネットワークもしくはホストのアドレスを記述するネットワークアドレスフィールド85と、各ネットワークもしく

6

はホスト毎のトラフィックの制限値を記述するトラフィック制限値フィールド86により構成されるレコードの集まりである。87はオープンファイル情報テーブルであり、計算機11の外部記憶装置210に格納されたファイル名を記述するファイル名フィールド88と、これらのファイルにアクセス可能なユーザのIDを記述するアクセスユーザフィールド89と、前記アクセスユーザがファイルにアクセスする際に使用するプログラムの名称を記述するプログラム名フィールド810により構成されるレコードの集まりである。内部状態定義テーブル21の設定内容は、ユーザが決定することができる。

【0021】外部からの侵入が発生したとき、ネットワークからのアクセスに対処するサービスを実現するプロセスに対して、(1)想定している以上の個数のプロセスが起動されたり、(2)プロセスが想定している以上の個数のパケットを受信したりする。また、特定のファイルシステムが想定外の利用者からアクセスされる場合がある。図8のテーブルの内容は、これらの事項をチェックすることにより、外部からの侵入を検出するためのものである。

【0022】図9は内部状態監視センサ部22からリソースアクセスコントロール部23および情報伝達部24に対して送信されるメッセージの構成例を示した図である。この例では、メッセージ91は、異常の種類を格納するフィールド92と、内部状態テーブルレコードデータを格納するフィールド93とを有する。フィールド92には、「プロセステーブル監視結果」、「ネットワークインタフェース監視結果」、「オープンファイル監視結果」のいずれかが格納される。フィールド93に格納される内部状態テーブルレコードデータは、プロセス数定義テーブル81、パケット数定義テーブル84、オープンファイル情報テーブル87のレコードのいずれかである。

【0023】図11に、プロセステーブル27の構成例を示す。これは、オペレーティングシステム26のカーネル内に常駐するテーブルであり、1レコードで1つのプロセスについての情報を保持する。このテーブル27は、使用情報271、スケジューリング情報272、資源利用状況に関する情報273、他プロセスへのポインタ274、テキスト構造体へのポインタ275、およびページテーブルへのポインタ27の各フィールドを有する。使用情報271は、個々のエントリ278が使用中か否かを示す情報であり、使用中の場合、そのプロセスの実行者(ユーザID)を示す。スケジューリング情報272は、そのプロセスが、「生成」、「実行中」、「待ち」、「実行可」のどの状態にあるかを示す情報である。資源利用状況に関する情報273は、そのプロセスが計算機の各入出力デバイスに対し、「使用中」、「待ち」、「その他」のどの状態にあるかを示す情報である。他プロセスへのポインタ274は、プロセスを実

行するために必要な他のプロセス（親プロセス、その他）を指し示すポインタである。テキスト構造体へのポインタ275は、他プロセスと共有可能なテキスト領域を指し示すポインタである。ページテーブルへのポインタ276は、仮想アドレスと実メモリとの対応関係を保持するテーブルのエントリを指し示すポインタである。本発明では、プロセステーブル27のエントリ数、および各エントリの使用情報271を利用することにより、各ユーザの使用プロセス数を把握する。また、「資源利用状況に関する情報273を利用することにより、例えば特定のデバイスへのアクセスを要求しているプロセス数を把握する。

【0024】図3は、図2に示した計算機において実行される、内部の監視による異常の検出および異常検出時の処理のフローチャートである。まず、内部状態監視センサ部21が監視データをオペレーティングシステム26から収集する（ステップ31）。ついで、取得した監視データを内部状態定義テーブル21のエントリと比較する（ステップ32）。ステップ32で比較した結果、異常があったかどうか判断する（ステップ33）。異常がなければ、最初のステップ31へ戻る。異常ありと判定された場合には、内部状態監視センサ部22よりリソースアクセスコントロール部23に異常の発生を通知する（ステップ34）。ステップ34の通知結果に基づきリソースアクセスコントロール部23がアクセスコントロール処理を実行する（ステップ35）。内部状態監視センサ部22は、また、情報伝達部24に異常の発生を通知する（ステップ36）。この通知を受けて、情報伝達部24は通信先一覧リスト25より異常の発生を知らせるメッセージの通知先他計算機を特定する（ステップ37）。そこで、情報伝達部24が他計算機12～15およびファイアウォール11に対して異常の発生を知らせるメッセージを送信する（ステップ38）。

【0025】図4は、図2に示した計算機において、他計算機が異常を検出したことに応答して行われる異常通知メッセージ受信時の処理のフローチャートである。情報伝達部24で他計算機からの異常を通知するメッセージを受信する（ステップ41）。このステップ41で受信したメッセージが正当な発信者により発信されたものか確認する（ステップ42）。不当と判断されれば、以後のステップを実行することなく本処理を終了する。正当と判断された場合、情報伝達部24よりリソースアクセスコントロール部23に他計算機で発生した異常を通知する（ステップ43）。この通知結果に基づき、リソースアクセスコントロール部23がアクセスコントロール処理および、実行中のジョブに対する制御を実行する（ステップ44）。本処理は特にファイアウォール11において実行することにより、計算機12～15に対するアクセスコントロール処理を一括して実行することができる。

【0026】図5は、内部状態監視センサ部22において、計算機11で実行中のプロセスの個数に着目した監視処理の一例を示すフローチャートである。まず、オペレーティングシステム26内のプロセステーブル27よりユーザIDごとに実行中のプロセス数を取得する（ステップ51）。次に、このステップで取得したユーザIDごとの実行プロセス数を、内部状態定義テーブル21に記述された当該ユーザIDのプロセス数の制限値と比較する（ステップ52）。いずれのユーザIDについても実行中プロセス数がその制限値を越えなければ、一定時間スリープする（ステップ53）。制限値を越えていた場合には、他の処理部および他の計算機へ通知するメッセージを組み立てる（ステップ54）。ついで、リソースアクセスコントロール部23にステップ54で作成したメッセージを送信する（ステップ55）。さらに、情報伝達部24にステップ54で作成したメッセージを送信する（ステップ56）。その後、ステップ51へ戻る。

【0027】図6は、内部状態監視センサ部22において、計算機11のネットワークインタフェース部のトラフィックに着目した監視処理を示すフローチャートである。まず、ネットワークアドレス毎に、オペレーティングシステムのネットワークドライバ28より単位時間あたりのパケット送受信数を取得する（ステップ61）。ついで、このステップ61で取得したパケット数を、ネットワークアドレス毎に、内部状態定義テーブル21に記述されたパケット数の制限値と比較する（ステップ62）。いずれのネットワークアドレスについても、制限値を越えていない場合には、一定時間スリープした後（ステップ63）、最初のステップ61へ戻る。いずれかのネットワークアドレスについて制限値を越えていた場合には、他の処理部および他の計算機へ通知するメッセージを組み立てる（ステップ64）。このステップ64で作成したメッセージをリソースアクセスコントロール部23に送信する（ステップ65）。さらに、情報伝達部24にもこのメッセージを送信する（ステップ66）。その後、ステップ61へ戻る。

【0028】図7は、内部状態監視センサ部22において、計算機11のローカルなファイルシステムに対し、ユーザプロセスで当該ファイルシステムへのアクセス要求が発生した時の監視処理を示すフローチャートである。まず、オペレーティングシステム26からのファイルシステムへのアクセス要求の発生の通知を待つ（ステップ71）。通知があれば、ファイルシステム制御システムコール29から、ファイルアクセスを要求したプロセスのIDおよび、アクセスされたファイルのIDが内部状態監視センサ部22に通知される。そこで、内部状態テーブル21のオープンファイル情報テーブル87を参照することにより、アクセスされたファイルが監視対象かどうか確認する（ステップ72）。監視対象でな

9

ければ、ステップ71へ戻る。監視対象であれば、ステップ71で取得したプロセスIDから利用者名および起動プログラム名称を割り出す(ステップ73)。このステップ73で割り出した利用者および起動プログラムが、内部状態定義テーブル21のオープンファイル情報テーブル87に記載されているものと一致するか(登録されているか)否かを確認する(ステップ74)。一致していれば、問題ないと判断して、最初のステップ71へ戻る。一致していなければ、他の処理部および他の計算機へ通知するメッセージを組み立てる(ステップ75)。ステップ75で作成したメッセージをリソースアクセスコントロール部23に送信する(ステップ76)。さらに、このメッセージを情報伝達部24に送信する(ステップ77)。その後、ステップ71へ戻る。

【0029】本方式のネットワークセキュリティシステムでは、計算機11の内部状態の監視処理を、図5から図7までの処理を組み合わせて行なう。

【0030】図10は、リソースアクセスコントロール部23において、内部状態監視センサ部22から通知

(メッセージ)を受信した時の処理を示すフローチャートである。まず、メッセージ91を受信する(ステップ101)。ついで、この受信したメッセージの異常種別92が「プロセステーブル監視結果」であるか否かを判定する(ステップ102)。そうでなければ、異常種別92が「ネットワークインタフェース監視結果」である

か否かを判定する(ステップ103)。ステップ102において異常種別92が「プロセステーブル監視結果」であると判定された場合、内部情報テーブルレコード格納フィールド93より当該異常と判定されたユーザのユーザIDを取得する(ステップ104)。ついで、当該ユーザのプロセスの起動制限をオペレーティングシステムに要求する(ステップ105)。例えば、オペレーティングシステム26は、ステップ104で取得したユーザIDを記憶する領域を持ち、新規プロセス生成時にその記憶領域と照合することにより、当該ユーザについては新たなプロセス生成を抑止する。ステップ103において、異常種別92が「ネットワークインタフェース監視結果」であると判定された場合、メッセージ91の内部情報テーブルレコード格納フィールド93より当該異常と判定されたネットワークアドレスを取得する(ステップ106)。

そこで、当該ネットワークアドレスからのアクセスを遮断するようネットワークインタフェースの設定を変更する(ステップ107)。例えば、オペレーティングシステムは、ネットワークインタフェースの入出力に対して、相手先アドレスによるフィルタリングの機能を持ち、当該ネットワークアドレスからの通信については入出力を抑止するようネットワークインタフェースの設定を変更する。ステップ103において、異常種別92が「ネットワークインタフェース監視結果」ではないと判定された場合は、メッセージ91の内部情報

10

テーブルレコード格納フィールド93よりファイル名を取得する(ステップ109)。そこで、このファイルのアクセスパーミッションを変更するようオペレーティングシステムに要求する(ステップ109)。オペレーティングシステムは、管理リソースに対するアクセス制御機能を有しており、例えばUNIXシステムの場合、個々のファイル単位でファイルのオーナーであるユーザ、オーナーの属するグループのユーザ、その他のユーザの3つのカテゴリに対して「読みとり」、「書き込み」、「実行」の権限を設定することができる。ここでは、グループもしくはその他のユーザに対する「読みとり」権限があったファイルをオーナーのみ読みとれるようにする変更、あるいは「書き込み」権限をすべて外すような変更を行う。監視による侵入の検出状況に応じて、段階的にアクセス制御を実施することも可能である。

【0031】以上、本発明の好適な実施の形態について説明したが、種々の変形・変更を行うことが可能である。例えば、ネットワークに接続した計算機において、監視の対象となるリソースを登録するテーブルの内容の更新時に、他の計算機にそのテーブルの内容を通知し、他の計算機は当該通知内容に基づき、自己の監視の対象となるリソースを登録するテーブルの内容を更新するような構成も可能である。

【0032】また、ネットワークに接続した計算機において、複数のサーバが連動することにより動作するサービス、例えばネットワークニュースやメールシステムが稼働しているネットワークシステムに対して、連係して侵入対策を行なうと共に、侵入対策に応じて連動サービスの動作を変更することも可能である。具体的には、ネットワークニュースのシステムは、ユーザが最寄りのニュースサーバに対して送信したニュース記事を、隣接するニュースサーバとの間で定期的に交換することにより、すべてのニュースサーバが同一のニュース記事をすべて保持するシステムである。このようなシステムでは、(1)1台のサーバで検出した異常を、ニュースシステムを利用することにより隣接するサーバに対して通知することができ、(2)異常を検出したサーバをシステム全体から分離し、残りのニュースサーバによりニュースシステムのサービスを続行するように設定を変更することが可能となる。

【0033】

【発明の効果】本発明によれば、ネットワークに接続した計算機において、ネットワークを経由した外部からの侵入に対して自計算機のアクセス制御を行うことと、周囲の計算機へ侵入検出を通知することにより、自組織内の計算機リソースの保護を行なうことができる。特にファイアウォールに対して侵入検出を通知することにより、自組織全体の計算機リソースの保護を一括して行なうこともできる。

【図面の簡単な説明】

10

20

30

40

50

12

対する異常通知処理、 37…通信相手先の特定処理、 38…他計算機に対する異常通知処理、 41…他計算機か

らの異常通知受信処理、42…受信メッセージの確認処理、43…リソースアクセスコントロール部に対する異

常通知処理、44…リソースアクセスコントロール処理、51…プロセス数取得処理、52…プロセス数比較

処理、53…スリープ処理、54…通知メッセージ組み立て処理、55…リソースアクセスコントロール部に対

する送信処理、56…情報伝達部に対する送信処理、61…送受信パケット数取得処理、62…パケット数比較

処理、63…スリープ処理、64…通知メッセージ組み立て処理、65…リソースアクセスコントロール部に対

する送信処理、66…情報伝達部に対する送信処理、7
1…オペレーティングシステムからの通知待ち処理、7

2…アクセスされたファイルが監視対象か確認する処理、73…利用者名、プログラム名割り出し処理、74

…利用社名、プログラム名が登録されているか確認する
処理、75…通知メッセージ組み立て処理、76…リソ

一 情報伝達部に対する送信処理、81…プロセス数定義テ

数制限値フィールド、84…パケット数定義テーブル、

【符号の説明】

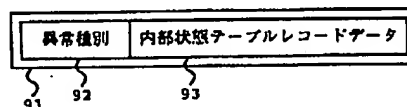
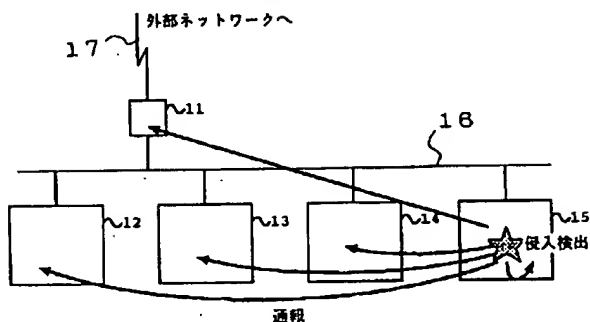
85…ネットワークアドレスフィールド、86…トラフィック制限値フィールド、87…オープンファイル情報テーブル、88…ファイル名フィールド、89…アクセスユーザフィールド、810…プログラム名フィールド、91…メッセージ、92…異常種別格納フィールド、93…内部状態テーブルレコードデータ格納フィールド、101…メッセージ受信処理、102…異常種別判定処理、103…異常種別判定処理、104…ユーザID取得処理、105…プロセス起動制限要求処理、106…ネットワークアドレス取得処理、107…ネットワーク経由アクセス遮断処理、108…ファイル名取得処理、109…アクセスパーミッション変更要求処理。

【図1】

【图9】

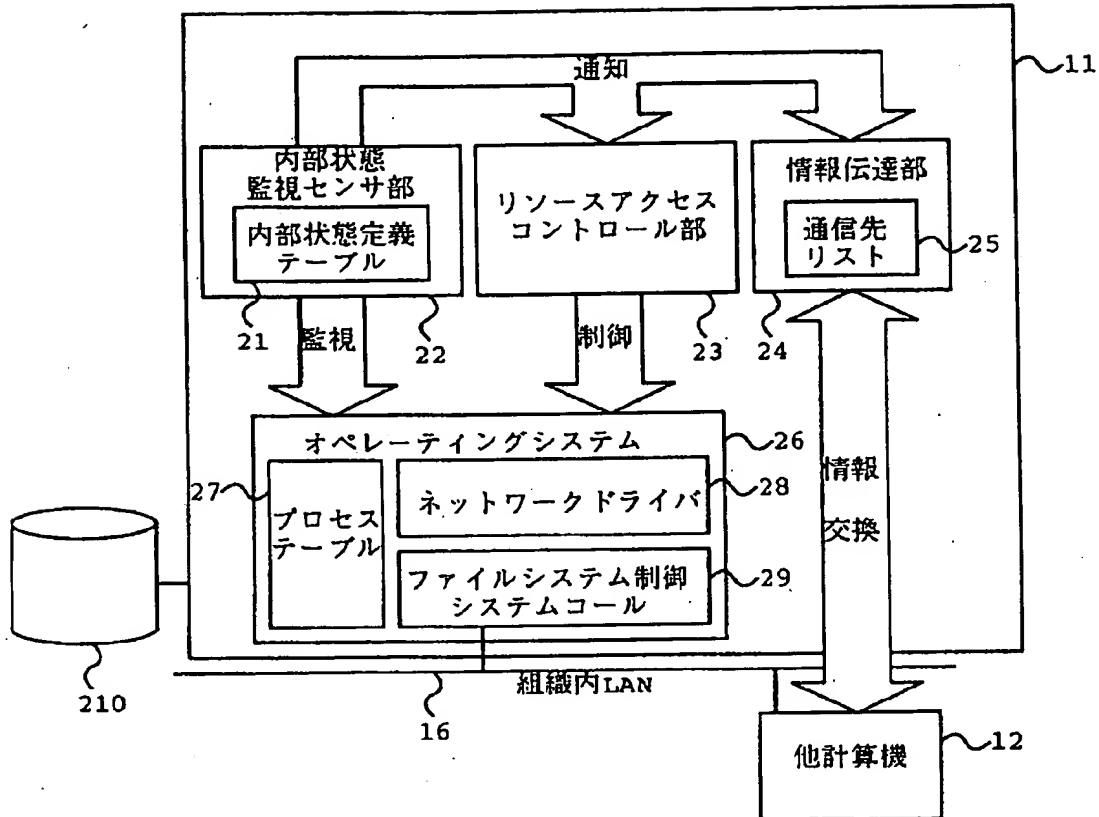
图 1

图 9



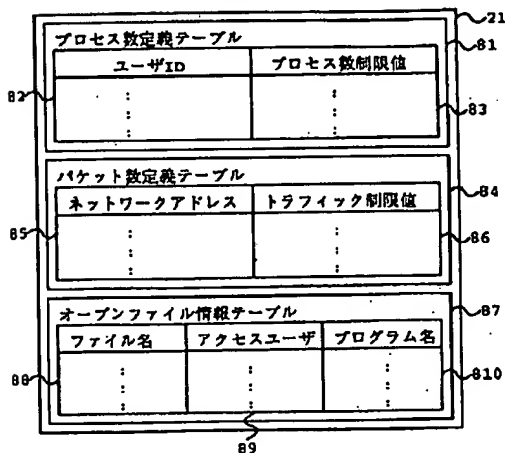
【図2】

図 2



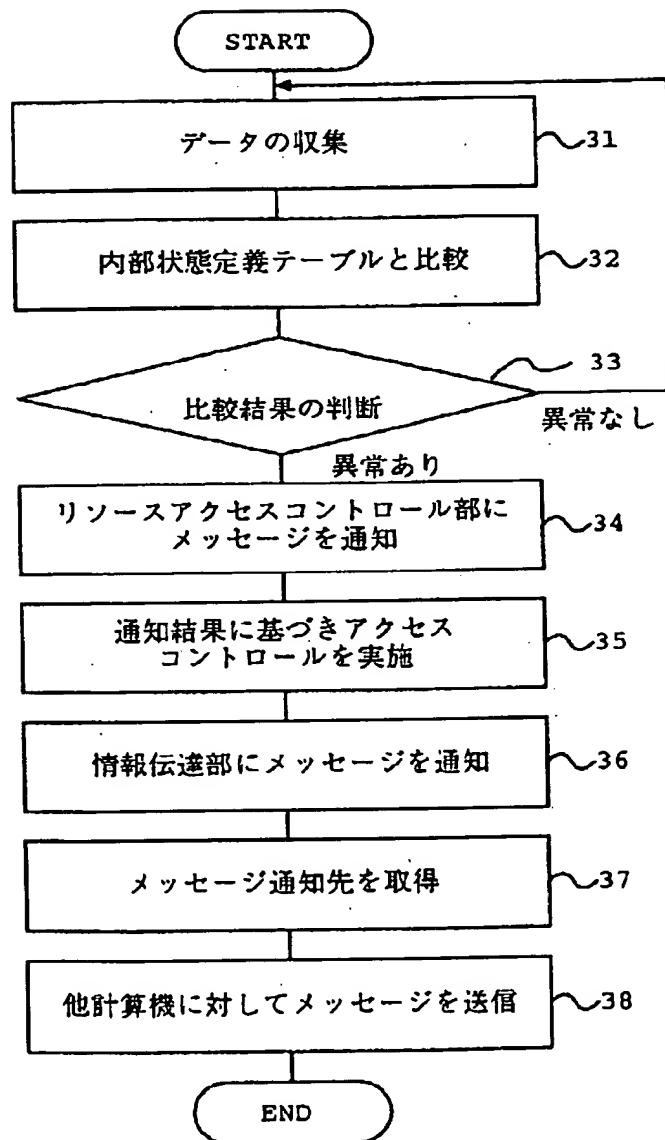
【図8】

図8



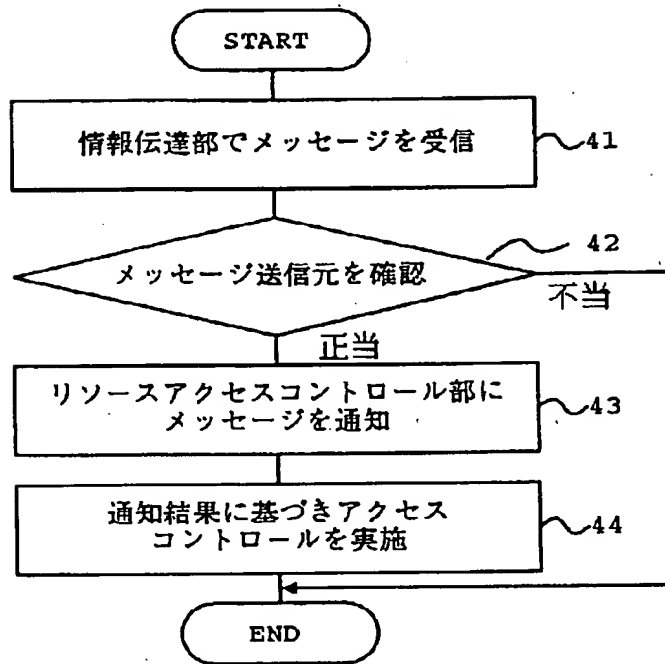
【図3】

図 3



【図4】

図 4



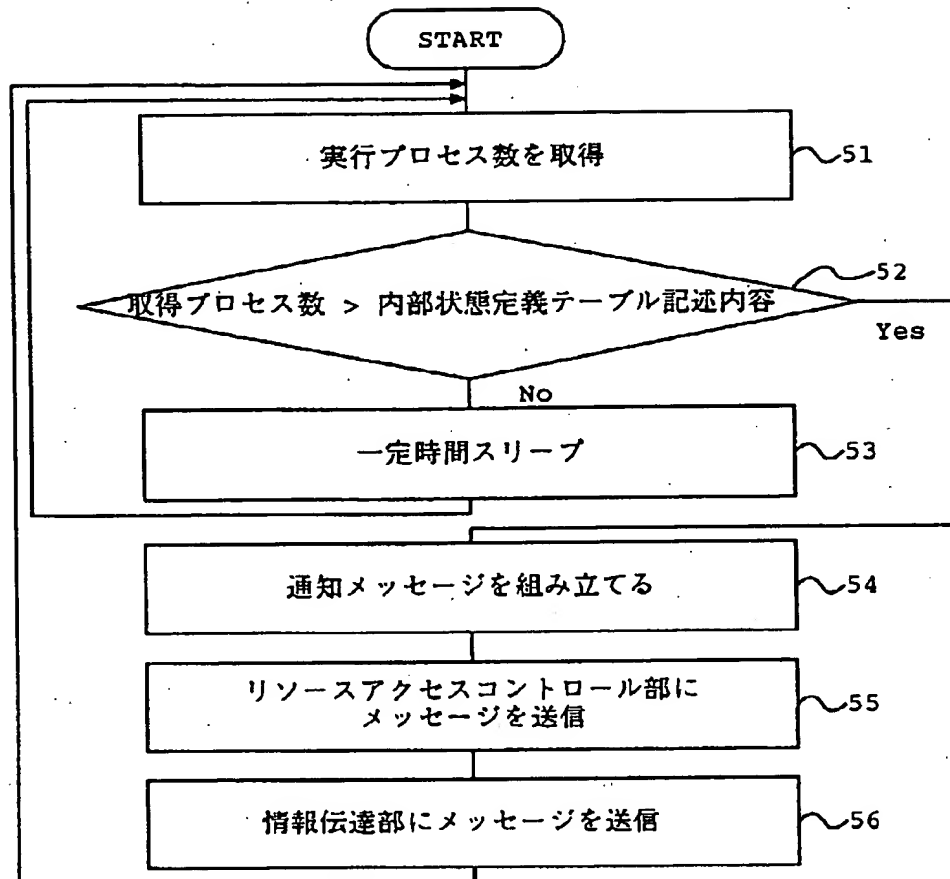
【図11】

図 11

271 使用 情報	272 スケジューリング 情報	273 資源利用状況 に関する情報	274 他プロセス へのポインタ	275 テキスト構造体 へのポインタ	276 ページテーブル へのポインタ	27 ポインタ
278						
!	!	!	!	!	!	!

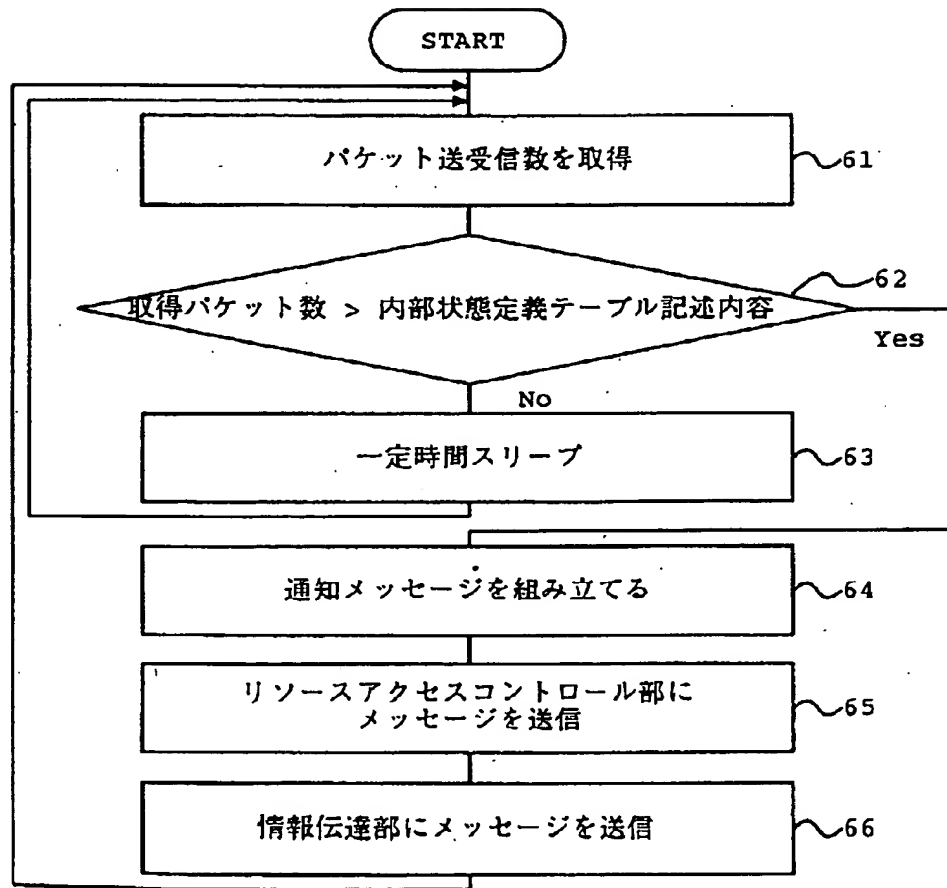
【図5】

図 5



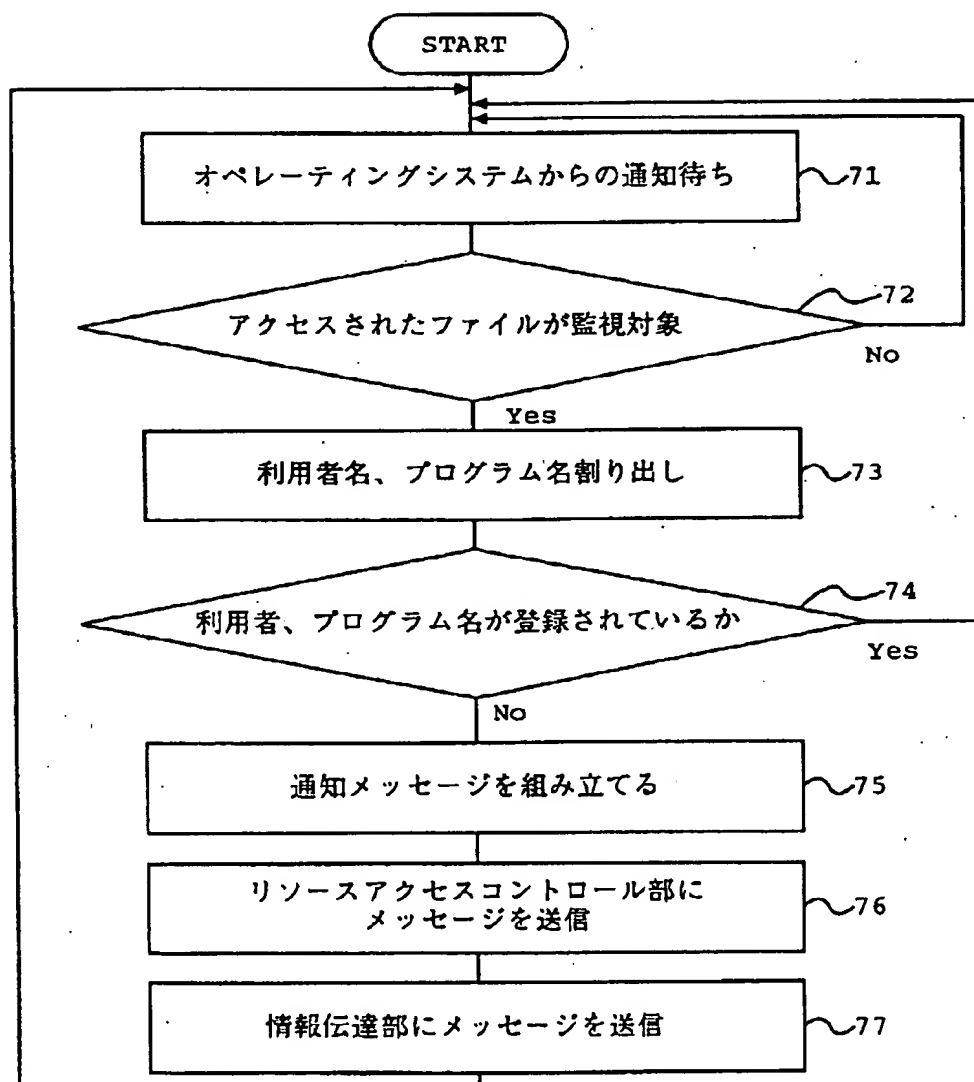
【図6】

図 6



【図7】

図 7



【図10】

図10

